PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-211932
(43)Date of publication of application : 17.09.1991

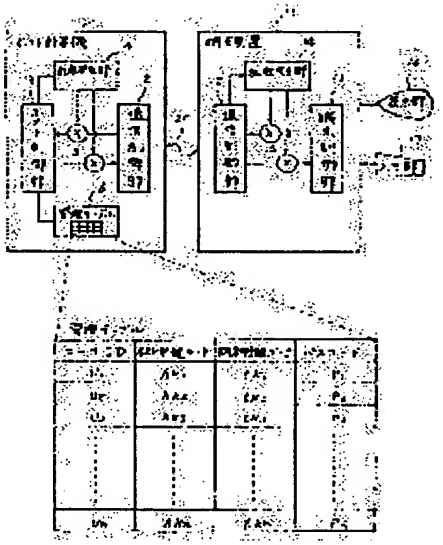
(51)Int.CI. H04L 9/00
G06F 15/00
G09C 1/00
H04L 9/10
H04L 9/12

(21)Application number : 02-006207
(22)Date of filing : 17.01.1990

(71)Applicant : HITACHI LTD
HITACHI MICRO SOFTWARE SYST CO LTD
(72)Inventor : NAKADA YUKIO
OKI TAKENORI

(54) COMMUNICATION CONTROL METHOD FOR DATA TERMINAL EQUIPMENT

(57)Abstract:
PURPOSE: To facilitate operations by eliminating the need for setting the key of telephone communication, etc., between a host and a terminal by executing batch control to the keys on a host side and a terminal side by the host side and automatically sending the key to be used by the terminal side from the host to the terminal at the time of log-ON from the terminal.
CONSTITUTION: The side of a host 1 executes the batch control to the keys to be used on the host 1 side and a terminal 11 side, and a means 3 is provided to automatically send the key to be used on the terminal 11 side form the host 1 to the terminal 11 at the time of log-ON from the terminal 11, to set the key and to update the key to be used on the host 1 side and the terminal 11 at every time. Thus, it is not necessary for the terminal 11 to set and control the key and the operation on the terminal 11 side is simplified. Further, by updating the keys on the host 1 side and the terminal 11 side every time, secrecy protection and safety can be secured.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of

rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3-211932

⑤Int.Cl.⁵	識別記号	庁内整理番号	㊸公開　平成3年(1991)9月17日
H 04 L 9/00 G 06 F 15/00 G 09 C 1/00 H 04 L 9/10 9/12	330 A	7218-5B 7230-5B	
		6914-5K　H 04 L 9/00　Z	

審査請求　未請求　請求項の数 1　(全4頁)

㊹発明の名称　データ端末装置の通信制御方法

㉑特　願　平2-6207
㉒出　願　平2(1990)1月17日

㉒発明者　中田　幸男　神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所マイクロエレクトロニクス機器開発研究所内
㉒発明者　沖　武則　神奈川県横浜市戸塚区吉田町292番地　株式会社日立マイクロソフトウエアシステムズ内
㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
㉑出願人　株式会社日立マイクロソフトウエアシステムズ　神奈川県横浜市戸塚区吉田町292番地
㉔代理人　弁理士　小川　勝男　外1名

明　細　書

1. 発明の名称

データ端末装置の通信制御方法

2. 特許請求の範囲

1. 端末装置とホスト計算機を通信回線で接続して暗号を用いた通信を行なうとき、ホスト側と端末側が同期して暗号鍵を設定し、暗号化する通信制御方式において、ホスト側がホスト側及び端末側が使用する鍵を一括管理し、端末からのログオン時に端末側が使用する鍵を自動的にホストから端末へ送り設定することと、毎回ホスト側及び端末側の鍵を更新する手段を持つことを特徴とするデータ端末装置の通信制御方法。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、端末装置を通信回線でホスト計算機と接続して暗号による通信を行なう上で、端末側の操作性向上及び従来通りの機密保護，安全性を確保する方法に関する。

〔従来の技術〕

従来，端末装置とホスト計算機を通信回線で接続して通信する上で暗号を使用する場合、ホスト側及び端末側ともに暗号に必要な鍵を電話連絡等で同期して設定する必要があった。

なお、関連する技術としては特開昭63-299546号が挙げられる。

〔発明が解決しようとする課題〕

端末装置とホスト計算機を通信回線で接続して暗号を用いた通信を行なうために、従来方式では、ホスト側と端末側が電話等で連絡し、暗号に必要な鍵を互に設定して使用していた。

本発明は、電話連絡等による鍵設定の手間を無くし、機密保護、安全性は従来通り確保できる手段を提供することを目的とする。

〔課題を解決するための手段〕

上記目的を達成するために、ホスト側がホスト側及び端末側が使用する鍵を一括管理し、端末からのログオン時に、端末側が使用する鍵を自動的にホストから端末へ送り設定する手段と、毎回ホスト側及び端末側が使用する鍵を更新する手段を

持つようにした。

〔作用〕

ホスト側がホスト側及び端末側が使用する鍵を一括管理し、端末からのログオン時に端末側で使用する鍵をホストから端末へ送り設定することにより、端末での鍵設定及び管理を無して端末側の操作を簡単にする。また、毎回（ログオンごとに）ホスト側及び端末側の鍵を更新することで機密保護、安全性を確保する。

〔実施例〕

以下、本発明の一実施例を図により説明する。第１図は本発明の一構成例を示し、１はホスト計算機、２は通信制御部、３はホスト制御部、４は乱数発生部、５は排他的論理和、６は管理テーブルである。

管理テーブルは、ユーザ番号ｉに対応するユーザＩＤUi、ホスト側鍵データhki、端末側鍵データtki、パスワードPiから構成されるテーブルである。各鍵データはユーザ番号ｉごとに異なる値に初期化されている。

第１図の１１は端末装置、１２は通信制御部、１３は端末制御部、１４は乱数発生部、１５は排他的論理和、１６は表示装置（ＣＲＴ）、１７は入力装置（キーボード）である。

なお、鍵データとは乱数発生部が乱数を発生するために必要な鍵（キー）である。

ホスト計算機と端末装置は通信回線２０により１対１に接続されている。

端末制御部１３の動作を第２図のフローチャートにより説明する。

端末制御部は、最初に乱数発生部の鍵データを初期化し、その後、キーボード１７からユーザＩＤを入力すると、そのユーザＩＤをホストへ送信する。

ホストからパスワード入力要求メッセージを受信すると、本メッセージ中に端末側鍵データが含まれているかチェックし、端末側鍵データが含まれているならば本メッセージから鍵データを分離して乱数発生部の鍵として設定する。

端末側鍵データが含まれていなければ、乱数発生部の鍵は初期化状態のままとする。

次にパスワード入力要求メッセージを表示部（ＣＲＴ）１６へ出力する。

パスワード入力要求メッセージに対し、キーボードからパスワードPn が入力されると、先に設定した端末側鍵データにより乱数発生部から発生される乱数とパスワードを排他的論理和を行ない暗号化し、ホストへ送る。

ホストから暗号化された応答を受信すると乱数発生部から発生する乱数と排他的論理和を行ない復号化してＣＲＴへ出力する。

応答が許可応答ならば通信を続行し、不許可応答ならば乱数発生部の鍵を初期化し、ユーザＩＤ入力にもどる。

ホスト制御部３の動作を第３図のフローチャートにより説明する。

ホスト制御部は端末装置からユーザＩＤUn を受けると、管理テーブル６からユーザＩＤに対応した端末側鍵データを求め、パスワード入力要求メッセージに付加して端末装置へ送る。なお、端末側鍵データがない場合は、パスワード入力要求メッセージのみ端末装置へ送る。

次に、管理テーブルからユーザＩＤに対応したホスト側鍵データを乱数発生部の鍵に設定し、管理テーブル中のホスト側及び端末側鍵データを更新する。

ホスト側鍵データがない場合は、乱数発生部の鍵は初期化状態のままとする。

暗号化されたパスワードを端末装置から受信すると先に設定されたホスト側鍵データにより乱数発生部から発生する乱数と排他的論理和をとり復号化する。

次にユーザＩＤに対応したパスワードを管理テーブルから求め、端末から受信したパスワードと比較し、一致すれば許可応答を不一致ならば不許可応答を乱数発生部から発生される乱数と排他的論理和を行ない暗号化して端末へ送る。

不許可の場合は、乱数発生部の鍵データを初期化して端末からの起動待ちとする。

鍵データが盗まれても、許可／不許可に関係な

く管理テーブル中のホスト側及び端末側鍵データを更新するため問題はない。

次にパスワード入力要求メッセージ中の鍵データを示すＥＳＣシーケンスを第４図に示す。

ＥＳＣ、ＴＫで端末側鍵データであることを示し、ｎは端末側鍵データ長を示して、その後に端末側鍵データがある。

パスワード入力要求メッセージ内の鍵データが盗まれても次回からは、鍵データは更新されているので使えない。また、鍵データにより暗号化されたパスワードが盗まれても、次回からは、その値は変れるので使えない。

〔発明の効果〕

本発明によれば、ホスト側がホスト側の鍵のみでなく端末側の鍵を一括管理し、端末からのログオン時に端末側が使用する鍵を自動的にホストから端末へ送ることにより、ホスト、端末間での電話連絡等による鍵設定を無すことができる。また、パスワード以降通信終了までの全てのデータを暗号化し、毎回（ログオンごとに）ホスト側及び端末側の鍵を更新することにより、データの機密保護、安全性を確保することができる。

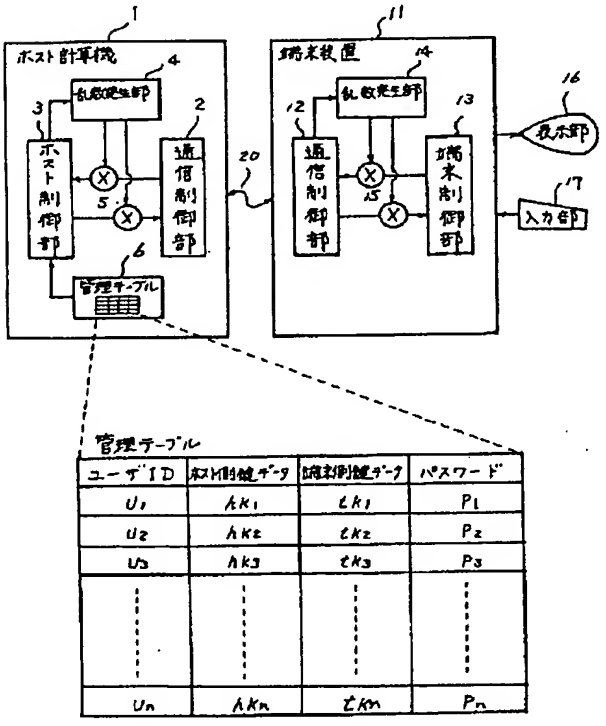
4. 図面の簡単な説明

第１図は本発明の一実施例の構成図、第２図は第１図の端末制御部の動作を示すフローチャート、第３図は第１図のホスト制御部の動作を示すフローチャート、第４図はパスワード入力要求メッセージ中に含まれる鍵データのフォーマット図である。

１…ホスト計算機、
２，１２…通信制御部、
３…ホスト制御部、
４，１４…乱数発生部、
５，１５…排他的論理和、
６…管理テーブル、
１１…端末装置、
１３…端末制御部、
１６…表示装置（ＣＲＴ）、
１７…入力装置（キーボード）。

代理人弁理士　小　川　勝　男

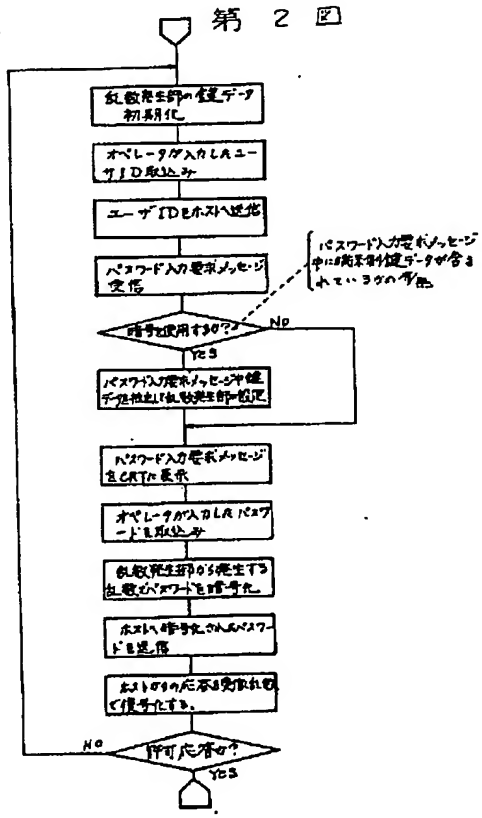
第１図



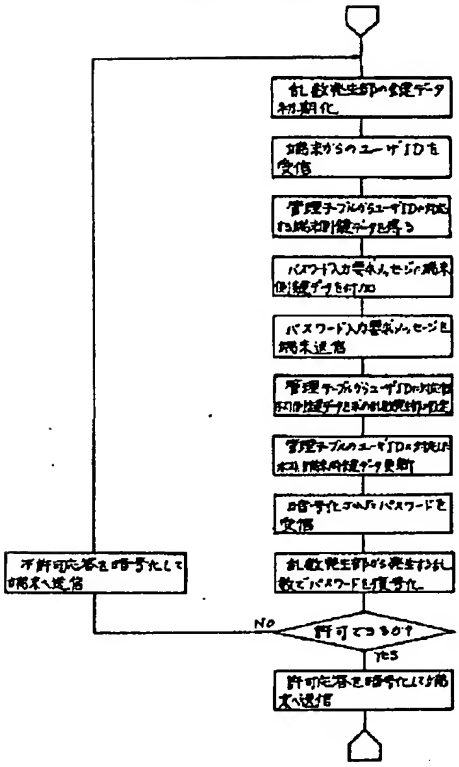
管理テーブル

ユーザID	ホスト側鍵データ	端末側鍵データ	パスワード
U_1	AK_1	tK_1	P_1
U_2	AK_2	tK_2	P_2
U_3	AK_3	tK_3	P_3
⋮	⋮	⋮	⋮
U_n	AK_n	tK_n	P_n

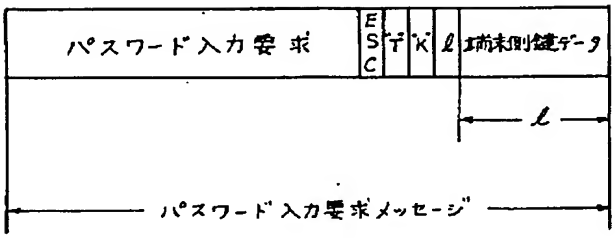
第２図



第 3 図



第 4 図



ESC：エスケープコード

TK　：端末側鍵データ識別コード

ℓ　　：端末側鍵データ長